UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/812,815	03/30/2004	Nikhil M. Deshpande	1000-0043	5073

7590 08/20/2008

The Law Offices of John C. Scott, LLC
c/o PortfolioIP
P.O. Box 52050
Minneapolis, MN 55402

EXAMINER	
REDDING, THOMAS M	
ART UNIT	PAPER NUMBER
2624	
MAIL DATE	DELIVERY MODE
08/20/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/812,815	DESHPANDE ET AL.	
	Examiner	Art Unit	
	THOMAS M. REDDING	2624	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 May 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22,46-50 and 57-60* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-22, 46-50 and 57-60* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *30 March 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Election/Restrictions

1. Applicant's election without traverse of Group I, consisting of claims 1-22, 46-50 and 57-60, in the reply filed on 5/6/2008 is acknowledged.

Specification

2. Applicant is reminded of the proper content of an abstract of the disclosure.

A patent abstract is a concise statement of the technical disclosure of the patent and should include that which is new in the art to which the invention pertains. If the patent is of a basic nature, the entire technical disclosure may be new in the art, and the abstract should be directed to the entire disclosure. If the patent is in the nature of an improvement in an old apparatus, process, product, or composition, the abstract should include the technical disclosure of the improvement. In certain patents, particularly those for compounds and compositions, wherein the process for making and/or the use thereof are not obvious, the abstract should set forth a process for making and/or use thereof. If the new technical disclosure involves modifications or alternatives, the abstract should mention by way of example the preferred modification or alternative.

The abstract should not refer to purported merits or speculative applications of the invention and should not compare the invention with the prior art.

Where applicable, the abstract should include the following:
(1) if a machine or apparatus, its organization and operation;
(2) if an article, its method of making;
(3) if a chemical compound, its identity and use;
(4) if a mixture, its ingredients;
(5) if a process, the steps.

Extensive mechanical and design details of apparatus should not be given.

The abstract in its current form is essentially a paraphrase of the title and gives little clue as to the nature of the invention. Correction is required.

3. The abstract of the disclosure is objected to because it has a title. Correction is required. See MPEP § 608.01(b).

> **(b) A brief abstract of the technical disclosure in the specification must commence on a separate sheet, preferably following the claims, under the heading "Abstract" or "Abstract of the Disclosure." The sheet or sheets presenting the abstract may not include other parts of the application or other material. The abstract in an application filed under 35 U.S.C. 111 may not exceed 150 words in length.**
> **The purpose of the abstract is to enable the United States Patent and Trademark Office and the public generally to determine quickly from a cursory inspection the nature and gist of the technical disclosure. (MPEP § 608.01(b))**

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

The USPTO "Interim Guidelines for Examination of Patent Applications for Patent Subject Matter Eligibility" (Official Gazette notice of 22 November 2005), Annex IV, reads as follows:

> Descriptive material can be characterized as either "functional descriptive material" or "nonfunctional descriptive material." In this context, "functional descriptive material" consists of data structures and computer programs which impart functionality when employed as a computer component. (The definition of "data structure" is "a physical or logical relationship among data elements, designed to support specific data manipulation functions." The New IEEE Standard Dictionary of Electrical and Electronics Terms 308 (5th ed. 1993).) "Nonfunctional descriptive material" includes but is not limited to music, literary works and a compilation or mere arrangement of data.
>
> When functional descriptive material is recorded on some computer-readable medium it becomes structurally and functionally interrelated to the medium and will be statutory in most cases since use of technology permits the function of the descriptive material to be realized. Compare In re Lowry, 32 F.3d 1579, 1583-84, 32 USPQ2d 1031, 1035 (Fed. Cir. 1994) (claim to data structure stored on a computer readable medium that increases computer efficiency held statutory) and Warmerdam, 33 F.3d at 1360-61, 31 USPQ2d at 1759 (claim to computer having a specific data structure stored in memory held statutory product-by-process claim) with Warmerdam, 33 F.3d at 1361, 31 USPQ2d at 1760 (claim to a data structure per se held nonstatutory).
>
> In contrast, a claimed computer-readable medium encoded with a computer program is a computer element which defines structural and functional interrelationships between the computer program and the rest of the computer which permit the computer program's functionality to be realized, and is thus statutory. See Lowry, 32 F.3d at 1583-84, 32 USPQ2d at 1035.

Claims 46- 50 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter as follows. Claim 46, and by dependency claims 47-50, defines an article comprising a storage medium embodying functional descriptive material (i.e., a computer program or computer executable code). However, the claim does not define a "computer-readable medium or computer-readable memory" and is thus non-statutory for that reason (i.e., "When functional descriptive material is recorded on some computer-readable medium it becomes structurally and functionally interrelated to the medium and will be statutory in most cases since use of technology permits the function of the descriptive material to be realized" – Guidelines Annex IV). The scope of the presently claimed invention encompasses products that are not necessarily computer readable, and thus NOT able to impart any functionality of the recited program. The examiner suggests amending the claim(s) to embody the program on "computer-readable medium" or equivalent; assuming the specification does NOT define the computer readable medium as a "signal", "carrier wave", or "transmission medium" which are deemed non-statutory (refer to "note" below). Any amendment to the claim should be commensurate with its corresponding disclosure.

Note:

"A transitory, propagating signal … is not a "process, machine, manufacture, or composition of matter." Those four categories define the explicit scope and reach of

subject matter patentable under 35 U.S.C. § 101; thus, such a signal cannot be patentable subject matter." (In re Nuijten, 84 USPQ2d 1495 (Fed. Cir. 2007). Should the full scope of the claim as properly read in light of the disclosure encompass non-statutory subject matter such as a "signal", the claim as a whole would be non-statutory. Should the applicant's specification define or exemplify the computer readable medium or memory (or whatever language applicant chooses to recite a computer readable medium equivalent) as statutory tangible products such as a hard drive, ROM, RAM, etc, **as well as** a non-statutory entity such as a "signal", "carrier wave", or "transmission medium", the examiner suggests amending the claim to *include* the disclosed tangible computer readable storage media, while at the same time *excluding* the intangible transitory media such as signals, carrier waves, etc.

Merely reciting functional descriptive material as residing on a tangible medium is not sufficient. If the scope of the claimed medium covers media other than "computer readable" media (e.g., "a tangible media", a "machine-readable media", etc.), the claim remains non-statutory. The full scope of the claimed media (regardless of what words applicant chooses) should not fall outside that of a computer readable medium.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –

(a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 1 is rejected under 35 U.S.C. 102(b) as being anticipated by Doyle et al. (US 2002/0095586).

Regarding claim 1, Doyle discloses [a] wireless device ("The present invention improves the security of wireless pervasive devices", Doyle, paragraph 46) comprising:

at least one biometric sensor to obtain biometric information about a user presently holding said wireless device when said wireless device is being held ("Yet another object of the present invention is to provide this continuous authentication using a biometric sensor", Doyle, paragraph 21);

a biometric authentication unit to determine, based on said biometric information, whether said user presently holding said wireless device is authorized to use said wireless device ("repeatedly obtaining, from the biometric sensor component, biometric input of a user of the computing device; and comparing the repeatedly obtained biometric input to the securely-stored biometric information of the owner, wherein each of the comparisons comprises an authentication of the user", Doyle, paragraph 24);

a wireless transceiver to support wireless communication with a remote entity ("radio transmitters", paragraph 56); and

a controller to control operation of said wireless device, wherein said controller is programmed to change operational characteristics of said wireless device based on whether said wireless device is presently being held ("If the authentication process of Block 220 completes successfully, then the security core may trust the application processor (and, inter alia, allow it to perform functions and exchange information with the I/O subsystem)", Doyle, paragraph 64, if the device is not being held, authentication won't occur and the security module will block functionality and "The buses 140, 160 are depicted as hardware buses, but they could also be implemented as wireless links, coupling the various I/O and application processor components with the security core wirelessly", Doyle, paragraph 50).

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 2-4, 6, 13-15, 17, 46 and 48 are rejected under 35 U.S.C. 103(a) as being unpatentable over Doyle et al. (US 2002/0095586).

Regarding claim 2, Doyle teaches wherein:

said controller is programmed to request access to a network, using said wireless

transceiver, and said biometric authentication unit indicates that said user presently holding said wireless device is authorized to use said wireless device ("If the authentication process of Block 220 completes successfully, then the security core may trust the application processor (and, inter alia, allow it to perform functions and exchange information with the I/O subsystem)", Doyle, paragraph 64, if the device is not being held, authentication won't occur and the security module will block functionality).

While Doyle does not explicitly disclose that access is requested when said wireless device is being held, Doyle does teach that his system requests access continuously by sending the biometric information of the user ("repeatedly obtaining, from the biometric sensor component, biometric input of a user of the computing device; and comparing the repeatedly obtained biometric input to the securely-stored biometric information of the owner, wherein each of the comparisons comprises an authentication of the user", Doyle, paragraph 24).

It would have been obvious at the time the invention was made to one of ordinary skill in the art that the continuous authentication of the user as taught by Doyle would be equivalent to an access request when the wireless device is being held.

Regarding claim 3, Doyle discloses wherein:

said controller includes information identifying said user presently holding said wireless

device as part of said request ("The comparison may alternatively be performed by the security component", Doyle, paragraph 29, and figure 1,reference 28 – biometric sensor communicates with the security component – reference 150 – security core, over I/0 bus – reference 140, which may be a wireless link, so user info must be passed in the request to the security core to authenticate).

Regarding claim 4, Doyle discloses wherein:

said controller includes biometric information obtained by said at least one biometric sensor as part of said request ("The comparison may alternatively be performed by the security component", Doyle, paragraph 29, and figure 1,reference 28 – biometric sensor communicates with the security component – reference 150 – security core, over I/0 bus – reference 140, which may be a wireless link, so user info must be passed in the request to the security core to authenticate).

Regarding claim 6, Doyle teaches wherein:

said controller is programmed to deactivate user functions of said wireless device when said wireless device is being held and said biometric authentication unit indicates that said user presently holding said wireless device is not authorized to use said wireless device ("The technique may further comprise aborting the security-sensitive operation if the repeated obtaining of biometric input or the comparison step fails to detect the biometric information of the user, thereby causing the completion of the security-sensitive operation", Doyle, paragraph 29).

Regarding claim 13, Doyle discloses wherein:

said controller is programmed to use readings of said at least one biometric sensor to determine whether said wireless device is currently being held ("repeatedly obtaining, from the biometric sensor component, biometric input of a user of the computing device; and comparing the repeatedly obtained biometric input to the securely-stored biometric information of the owner, wherein each of the comparisons comprises an authentication of the user", Doyle, paragraph 24).

Regarding claim 14, Doyle discloses wherein:

said at least one biometric sensor includes at least one of the following: a fingerprint sensor, a skin temperature sensor, a skin texture sensor, a hand geometry sensor, a voice print sensor, and a heartbeat sensor ("The biometric sensor component may be: a fingerprint sensor (in which case the fingerprint sensor is capable of repeatedly obtaining a fingerprint of the user as the biometric input of the user while the computing device is being held by the user); a retina scanner (in which case the retina scanner is capable of repeatedly obtaining a retinal scan of the user as the biometric input of the user while the user is looking at the computing device); or any other biometric sensor", Doyle, paragraph 28).

Regarding claims 15 and 46 Doyle discloses [a] method comprising:

sensing that a wireless device has been picked up by a user;

determining, after sensing that said wireless device has been picked up, whether said user is authorized to use said wireless device based on collected biometric information ("repeatedly obtaining, from the biometric sensor component, biometric input of a user of the computing device; and comparing the repeatedly obtained biometric input to the securely-stored biometric information of the owner, wherein each of the comparisons comprises an authentication of the user", Doyle, paragraph 24); and when said user is determined to be authorized to use said wireless device, requesting access to a network via a wireless link ("If the authentication process of Block 220 completes successfully, then the security core may trust the application processor (and, inter alia, allow it to perform functions and exchange information with the I/O subsystem)", Doyle, paragraph 64, if the device is not being held, authentication won't occur and the security module will block functionality and "The buses 140, 160 are depicted as hardware buses, but they could also be implemented as wireless links, coupling the various I/O and application processor components with the security core wirelessly", Doyle, paragraph 50).

Further regarding claim 46, Doyle discloses [a]n article comprising a storage medium having instructions stored thereon ("the present invention provides a method, system, and computer program product for improving security of a computing device", Doyle , paragraph 35) that, when executed by a computing platform, operate to implement the method of claim 15 (as described above).

Regarding claims 17 and 48, Doyle discloses when said user is determined to not be authorized to use said wireless device, de-activating user functions of said wireless device ("The technique may further comprise aborting the security-sensitive operation if the repeated obtaining of biometric input or the comparison step fails to detect the biometric information of the user, thereby causing the completion of the security-sensitive operation", Doyle, paragraph 29).

Regarding claim 20, Doyle discloses when access to said network has been granted, allowing said user to perform network based functions ("If the comparison succeeds until completion of the security-sensitive operation, then the technique may further comprise concluding that the security-sensitive operation is authentic. This conclusion may also require that all other components which are securely operably connected to the security core remain securely operably connected until completion of the security-sensitive operation, or that all other components which are securely operably connected to the security core and which are involved in the security-sensitive operation remain securely operably connected until completion thereof", Doyle, paragraph 30, if user is authenticated, then he is given access to the security sensitive functions of networked devices).

8. Claims 5 and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Doyle et al. (US 2002/0095586) in combination with Loveland (US 2003/0070091).

Regarding claims 5, 21 and 22 Doyle teaches [t]he wireless device of claim 2.

Doyle does not teach, wherein: said controller is programmed to prompt said user presently holding said wireless device when network access has been denied.

Loveland, working in the same area of endeavor of controlling network access, does teach wherein: said controller is programmed to prompt said user presently holding said wireless device when network access has been denied ("When access rights are granted or revoked, a user associated with a user session may be so notified", Loveland, paragraph 14).

It would have been obvious at the time the invention was made for one of ordinary skill in the art to use the notification method taught by Loveland in the network authentication system of Doyle to make a user aware of his current access rights.

Regarding claim 22, Doyle teaches the method of claim 15 as given above.

Doyle does not teach when access to said network has been denied, allowing said user to perform local functions, but not network based functions.

Loveland, working in the same field of endeavor of controlling network access does teach when access to said network has been denied, allowing said user to perform local functions, but not network based functions ("The amount of access to network resources granted to different authentication methods may be predefined. For example,

a corporate information technology department may wish to manage authentication methods by assigning different levels of access to different authentication methods", Loveland, paragraph 12, Loveland teaches granting different levels of access based on authentication).

9. Claims 7, 8,16 and 47 are rejected under 35 U.S.C. 103(a) as being unpatentable over Doyle et al. (US 2002/0095586) in combination with Bi et al. (US 7,113,173).

Regarding claim 7 Doyle teaches [t]he wireless device of claim 1 as give above.

Doyle does not teach wherein:
said controller is programmed to place said wireless device in a power save mode when said wireless device is not being held.

Bi, working in the same problem solving area of power management in battery powered devices does teach wherein:
said controller is programmed to place said wireless device in a power save mode when said wireless device is not being held ("In this state 162, specific inactive devices are each put into a static state after a predetermined time-out period of inactivity for that device", Bi, column 8, line 57, if the device is not being held, it is not being used).

It would have been obvious at the time the invention was made for one of ordinary skill in the art to use a power management strategy as taught by Bi, in the network authentication system of Doyle “In order to conserve battery power” (Bi, column 8, line 39).

Regarding claim 8, the combination of Doyle and Bi teaches wherein:
said controller is programmed to place said wireless device in a normal power mode when said wireless device is being held (“These devices emerge from the static state once an activity relevant to its operation is detected, e.g. a pen event is detected”, Bi, column 9, line 2, detecting activity triggers return to normal power mode).

Regarding claims 16 and 47, the combination of Doyle and Bi teaches enabling a normal power mode of said wireless device after sensing and before determining (“These devices emerge from the static state once an activity relevant to its operation is detected, e.g. a pen event is detected”, Bi, column 9, line 2, and Doyle figure 1 and 4, Doyle indicates that bus 140 may be physical or wireless. “the validation may be performed by the security core 150 after securely transferring or accessing the information from the user's smart card”, If verification is via the security core and bus 140 is wireless it would be necessary to provide normal power to the transmitter to do the authentication).

10. Claims 9, 18 and 49 are rejected under 35 U.S.C. 103(a) as being unpatentable over Doyle et al. (US 2002/0095586) in combination with Knouse et al. (US 2003/0074580).

Regarding claims 9, 18, 19, 49 and 50 Doyle discloses all the elements of the parent claims 1, 15 and 46 as given above.

Doyle does not disclose a storage medium to store user profiles for multiple authorized users of said wireless device, wherein said controller loads a profile corresponding to said user presently holding said wireless device from said storage medium into a processor memory after said biometric authentication unit indicates that said user presently holding said wireless device is authorized to use said wireless device.

Knouse does teach a storage medium to store user profiles for multiple authorized users of said wireless device (Knouse figures 1 and 3, user profiles – 102 are stored on the directory server – 36) , wherein said controller loads a profile corresponding to said user presently holding said wireless device from said storage medium into a processor memory after said biometric authentication unit indicates that said user presently holding said wireless device is authorized to use said wireless device (“After authenticating the user, Web Gate 28 queries Access Server 34 about whether the user is authorized to access the resource requested. Access Server 34 in

turn queries Directory Server 36 for the appropriate authorization criteria for the requested resource", Knouse, paragraph 99).

It would have been obvious at the time the invention was made for one of ordinary skill in the art to combine the profile/policy system taught by Knouse in the network authentication system of Doyle to streamline controlling the access of multiple users with different access requirements (Knouse paragraphs 9-11).

Regarding claims 19 and 50, the combination of Doyle and Knouse teaches further comprising: when access to said network has been granted, loading a profile associated with said user into a processor memory ("After authenticating the user, Web Gate 28 queries Access Server 34 about whether the user is authorized to access the resource requested. Access Server 34 in turn queries Directory Server 36 for the appropriate authorization criteria for the requested resource", Knouse, paragraph 99, Knouse's server is accessed over the network).

11. Claims 10 and 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Doyle et al. (US 2002/0095586) in combination with Reisman (US 6,769,009 hereafter referred to as Reisman'009).

Regarding claim 10, Doyle teaches all the elements of claim 1 as given above.

Doyle does not teach wherein:

said controller is programmed to request access to a network for use in performing background functions, using said wireless transceiver, when said wireless device is not being held and when power is sufficient to perform said background functions.

Reisman'009 working in the same field of endeavor of network communications does teach wherein: said controller is programmed to request access to a network for use in performing background functions ("Information transport component 14 implements any necessary pre-transport preparation 104 and then, employing its own communications module 36, and server fetch-send protocol 44, proceeds in unattended mode, without requiring user intervention to establish call connection 60, to execute transport object 62 and automatically perform a disconnect 64, as described herein", Reisman'009, column 16, line 1), using said wireless transceiver, when said wireless device is not being held ("unattended mode", Reisman'009, column 16, line 5) and when power is sufficient to perform said background functions (if power is insufficient to perform the background tasks, then they can't be performed).

Regarding claim 11, the combination of Doyle and Reisman'009 teaches wherein:

said controller is programmed to enable performance of background functions after network access has been obtained ("Information transport component 14 implements any necessary pre-transport preparation 104 and then, employing its own communications module 36, and server fetch-send protocol 44, proceeds in unattended

mode, without requiring user intervention to establish call connection 60, to execute transport object 62 and automatically perform a disconnect 64, as described herein", Reisman'009, column 16, line 1, the actual fetch-send operation cannot occur until connection has been established).

12. Claim 12 is rejected under 35 U.S.C. 103(a) as being unpatentable over Doyle et al. (US 2002/0095586) in combination with Reisman (US 2003/0229900, hereafter referred to as Reisman'900).

Regarding claim 12, Doyle teaches all the elements of claim 1 as given above.

Doyle does not teach an accelerometer to monitor movement of said wireless device, wherein said controller is programmed to use readings of said accelerometer to determine whether said wireless device is currently being held

Reisman'900 does teach an accelerometer to monitor movement of said wireless device, wherein said controller is programmed to use readings of said accelerometer to determine whether said wireless device is currently being held ("Such states might be determined through sensing of motion change, such as by accelerometer, to rest on a fixed table or back to hand -held", Reisman'900, paragraph 705).

It would have been obvious at the time the invention was made for one of ordinary skill in the art to use the accelerometer motion sensing elements taught by Reisman'900 with the network authentication system of Doyle to "to anticipate and be responsive to the user's desires (and the author's suggestions) as to what resources to present where, in order to make the best possible use of the hardware resources at a user's disposal" (Reisman'900, paragraph 24, Reisman is teaching letting the system determine some behavior via the context of the device rather than through explicit user command).

13. Claim 57 is rejected under 35 U.S.C. 103(a) as being unpatentable over Doyle et al. (US 2002/0095586) in combination with Hayes et al. (US 5,949,383).

Regarding claim 57, Doyle teaches all the elements that are common with claim 1 as given above.

While Doyle does teach an antenna (Doyle, paragraph 56), Doyle does not explicitly give any details of his antenna.

Hayes, working in the same problem solving area of wireless communications does teach at least one dipole antenna coupled to said wireless transceiver to provide a transition to free space ("Accordingly, low-cost, lightweight, high-performance antennas may be provided, for example for cellular communication systems that are currently

being integrated into various platforms including Personal Digital Assistants (PDA) and laptop computers. A balanced antenna, such as a dipole, may be used in these noisy environments to provide balanced noise rejection capabilities", Hayes, column 5, line 3).

It would have been obvious at the time the invention was made for one or ordinary skill in the art to provide a dipole antenna as taught by Hayes in the network authentication system of Doyle to gain the advantages of low-cost, lightweight and high performance that is also capable of noise rejection in noisy environments (Hayes, column 5, line 3).

Regarding claim 58, the combination of Doyle and Hayes teaches wherein: said controller is programmed to request access to a network, using said wireless transceiver, and said biometric authentication unit indicates that said user presently holding said wireless device is authorized to use said wireless device.

While the combination of Doyle and Hayes does not explicitly teach that access is requested when said wireless device is being held, Doyle does teach that his system requests access continuously by sending the biometric information of the user ("repeatedly obtaining, from the biometric sensor component, biometric input of a user of the computing device; and comparing the repeatedly obtained biometric input to the securely-stored biometric information of the owner, wherein each of the comparisons comprises an authentication of the user", Doyle, paragraph 24).

It would have been obvious at the time the invention was made to one of ordinary skill in the art that the continuous authentication of the user as taught by Doyle would be equivalent to an access request when the wireless device is being held.

14. Claims 59 and 60 are rejected under 35 U.S.C. 103(a) as being unpatentable over Doyle et al. (US 2002/0095586) and Hayes et al. (US 5,949,383) in combination with BI et al. (US 7,113,173).

Regarding claim 59, the combination of Doyle and Hayes teaches [t]he wireless device of claim 57 as give above.

The combination of Doyle and Hayes does not teach wherein:
said controller is programmed to place said wireless device in a power save mode when said wireless device is not being held.

Bi, working in the same problem solving area of power management in battery powered devices does teach wherein:
said controller is programmed to place said wireless device in a power save mode when said wireless device is not being held (“In this state 162, specific inactive devices are

each put into a static state after a predetermined time-out period of inactivity for that device", Bi, column 8, line 57, if the device is not being held, it is not being used).

It would have been obvious at the time the invention was made for one of ordinary skill in the art to use a power management strategy as taught by Bi, in the network authentication system of Doyle and Hayes "In order to conserve battery power" (Bi, column 8, line 39).

Regarding claim 60, the combination of Doyle, Hayes and Bi teaches wherein: said controller is programmed to place said wireless device in a normal power mode when said wireless device is being held ("These devices emerge from the static state once an activity relevant to its operation is detected, e.g. a pen event is detected", Bi, column 9, line 2, detecting activity triggers return to normal power mode).

Conclusion

15. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Black essentially teaches all the elements of claim 1 with the exception of describing a transceiver, which is inherent to a wireless device.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to THOMAS M. REDDING whose telephone number is (571)270-1579. The examiner can normally be reached on Mon - Fri 7:30 am - 5:00 pm EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Vikkram Bali can be reached on (571) 272-7415. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/T. M. R./
Examiner, Art Unit 2624

/Vikkram Bali/
Supervisory Patent Examiner, Art Unit 2624